UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* the person of Jonathan Alvin AGUILLON, date of birth March 31, 1983, California driver's license number D1139729	)	Case No. 2:18-MJ-3232

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-2

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-2

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Sections 2252A(a)(2) , 2252A(a)(5)(B)	receipt and distribution of child pornography; access with intent to view and possession of child pornography

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

James DeCello, Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and state: Los Angeles, California

Hon. Charles Eick, United States Magistrate Judge

Printed name and title

AUSA: Joseph Axelrad, x7964

ATTACHMENT A-2

PERSON TO BE SEARCHED

The person to be searched, and the property that is on his person, is identified as Jonathan Alvin AGUILLON, date of birth March 31, 1983, California driver's license number D1139729, and any property including digital devices on his person, including, but not limited to, any pockets in his clothing, and any bags or other containers carried or held by him, provided that he is located within the Central District of California at the time of the search.

ATTACHMENT B-2

I. ITEMS TO BE SEIZED

1. Evidence, contraband fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (access with intent to view and possession of child pornography), specifically:

a. Child pornography, as defined in 18 U.S.C. § 2256(8).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including but not limited to documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256.

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Any and all records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertains to email address "yearofthebore@gmail.com."

g. Any documents, programs, applications, or materials, including electronic mail and electronic messages, that pertains to opening, closing, updating, and/or maintaining accounts with any Internet Service Provider.

h. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages,

regarding ownership and/or possession of the SUBJECT PREMISES, as defined in Attachment A-1.

i. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession and/or use of any digital device(s) found on the person of AGUILLON.

j. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

k. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing

data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, flash or thumb drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

I. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date

of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other

evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the

device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, James DeCello, being duly sworn, declare and state as follows:

I. BACKGROUND FOR TFO DECELLO

1. I am an Officer of the California Highway Patrol ("CHP") and have been so employed since April 2000. I am currently assigned as a Task Force Officer ("TFO") with the Federal Bureau of Investigation ("FBI"), Los Angeles Field Office, where I have been working in the Violent Crimes Against Children Squad since August 2018. In that capacity, I am assigned to the Southern California Regional Sexual Assault Felony Enforcement ("SAFE") Team, a multi-agency child exploitation task force, as well as the Los Angeles Innocence Lost Child Prostitution Task Force ("ILTF"). The SAFE Team is responsible for enforcing federal criminal statutes including the sexual exploitation of children under Title 18, United States Code, Section 2251, et seq. I have received specialized training in the areas of computer forensics, the Internet, and the storage and distribution of child pornography. The training has been provided by on the job training at the FBI as well as numerous civilian agencies and training schools.

2. As part of my training as a member of the SAFE Team and ILTF, I have consulted with colleagues who have many years

of experience investigating child prostitution, child pornography, and child exploitation cases. I have also been involved in the execution of numerous search warrants related to various crimes, including child pornography and child prostitution offenses.

3. Through both my training and my experience, I have become familiar with the methods of operation used by people who commit offenses involving the sexual exploitation of children and how people use the Internet to commit crimes arising from, and related to, the sexual exploitation of children.

II. PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of an application for a warrant to search:

a. The property located at 432 North Euclid Avenue, Apartment #3, in Pasadena, California (the "SUBJECT PREMISES"), as described further below and in Attachment A-1, which is incorporated herein by reference.

b. The person of Jonathan Alvin AGUILLON ("AGUILLON"), date of birth March 31, 1983, as described further in Attachment A-2, which is incorporated herein by reference, provided that AGUILLON is located within the SUBJECT PREMISES or the Central District of California at the time of the search.

5. As described more fully below, I respectfully submit there is probable cause to believe that the SUBJECT PREMIES and

the person of AGUILLON contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (access with intent to view and possession of child pornography) (collectively, the "SUBJECT OFFENSES"), as described further in Attachment B-1 and B-2, which are also incorporated herein by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. DEFINITIONS

7. The following terms, as used in this affidavit, have the following meanings:

a. "Minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256(8).

b. "Child erotica" means materials or items that are sexually arousing to persons who have a sexual interest in

minors, but that are not legally obscene or do not necessarily depict minors in sexually explicit conduct.

c. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

d. "Internet" is defined as the worldwide network of computers – a noncommercial, self-governing network devoted mostly to communication and research with billions of users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. To access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider, which operates a host computer with direct access to the Internet.

e. "Internet Protocol Address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses can also be "static," if an ISP assigns a user's computer a particular IP address that is

Instrumentality Protocol

used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

f. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

g. "Hyperlink" refers to an item on a webpage which, when selected, transfers the user directly to another location in a hypertext document or to some other webpage.

h. "Chat" means any kind of communication over the Internet that consists of the real-time transmission of messages between two or more users. Chat messages enable participants to respond quickly to one another and in a format that is similar to an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and e-mail.

A. THE USE OF PEER-TO-PEER FILE SHARING SOFTWARE TO DISTRIBUTE CHILD PORNOGRAPHY ON THE BITTORRENT NETWORK

8. Based on my training and experience in the investigations of child pornography and with Peer-to-Peer ("P2P") file sharing networks, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about P2P

Instrumentality Protocol

file sharing networks, including the BitTorrent P2P network, and child pornography:

a. Millions of computer users throughout the world use P2P file sharing networks to share files containing music, graphics, movies, and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the Internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

b. The BitTorrent network is a popular and publically available P2P file sharing network. Most computers that are part of this network are referred to as "peers" or "clients." A peer/client can simultaneously provide files to some peers/clients, while downloading files from other peers/clients.

c. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, uTorrent client program, and Vuze client program, among others. These client programs are publicly available, typically free, and can be downloaded from the Internet.

d. During the installation of typical BitTorrent client programs, various settings are established which

Instrumentality Protocol

configure the host computer to share files via automatic uploading. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding."

e. Files or sets of files are shared on the BitTorrent network via the use of "Torrents." A "Torrent" is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but instead contain information about the file(s) to be shared that is needed to accomplish a download. This information includes things such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent." The "info hash" is a SHA-1 hash value of the set of data describing the file(s) referenced in the "Torrent." This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent"

Instrumentality Protocol

file may also contain information on how to locate files referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the "Torrent." "Trackers" do not actually have the file(s). Instead, they are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. The use of "Trackers" on the BitTorrent network is not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

f. In order to locate "Torrent" files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include "isohhunt.com" and "piratebay.org." Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrent" files that describe the files they are looking to download. "Torrent" indexing websites do not actually host the content (files) described by "Torrent" files, only the "Torrent" files

Instrumentality Protocol

themselves. Once a "Torrent" file is located on the website that meets a user's keyword search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported that they have the same file(s) available for sharing (based on SHA1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent," to include the remote peers/clients' IP addresses.

g. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex," "pthc," or a specific age. The results of the keyword search are typically returned to the user's computer by displaying them on the "Torrent" indexing website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to download

Instrumentality Protocol

to their computer from the website. Typically, the BitTorrent client program will then process the "Torrent" file. Utilizing trackers and other BitTorrent network protocols, peers/clients are located that have recently reported that they have the file(s), or parts of the file(s), referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files. Typically, once the BitTorrent client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has downloaded with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA1 hash value of that piece which is described in the "Torrent" file. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the "Torrent" file, will remain in that location until moved or deleted by the user.

h. Law enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. By searching the network for child pornography-related "Torrents," law enforcement can quickly identify targets in the

Instrumentality Protocol

searcher's jurisdiction. Law enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network recently reporting that they are involved in sharing digital files of known or suspected child pornography, based on "info hash" SHA1 hash values of "Torrents." The "Torrents" being searched for are those that have been previously identified by law enforcement as being associated with such files. Additionally, there is law enforcement-specific BitTorrent network software which allows for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address, as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

i. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program that they are querying and/or downloading a file from. This information includes:

i. the suspect client's IP Address;

ii. a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in

Instrumentality Protocol

part, and that the pieces of the file(s) are being reported as shared from the suspect client program; and

the BitTorrent network client program and version being utilized by the suspect computer. Law enforcement has the ability to log this information.

j. The investigation of P2P file-sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of whom were also involved in the sexual exploitation of child victims.

IV. SUMMARY OF PROBABLE CAUSE

9. On April 29, 2017, January 22, 2018, and February 24, 2018, law enforcement officers, working in an undercover capacity, used BitTorrent to download files of suspected child pornography from a computer device connected to the Internet via IP address 75.27.242.239 (the "SUSPECT IP ADDRESS"). These images of suspected child pornography were publicly available for download to any Internet user with compatible peer-to-peer file-sharing software, which is available for free over the Internet. Further investigation revealed that at the times law

Instrumentality Protocol

enforcement officers downloaded the suspected child pornography, the IP Address was assigned to the SUBJECT PREMISES and was subscribed to AGUILLON. Subsequent investigation confirmed that AGUILLON lives at the SUBJECT PREMISES.

V. PROBABLE CAUSE

A. April 29, 2017 Download of Suspected Child Pornography from the SUSPECT IP ADDRESS

10. On or about August 15, 2018, I reviewed the report of an Undercover Law Enforcement Agent (hereafter, "UCA"), who, at the time of the investigation, was based in Tulsa, Oklahoma. The report documented the UCA's online covert investigation into the sharing of child pornography files over the BitTorrent P2P network on April 29, 2017. Based upon my review of this report, I know the following:

a. On April 29, 2017, the UCA saw a BitTorrent user connected to the BitTorrent network using the SUSPECT IP ADDRESS had made available for sharing the infohash: 817e0637dd4bdfdb4bc032408da650391d8fd609.[1] This torrent referenced 2,809 files, at least one of which was identified as being suspected child pornography

[1] Infohash or Hash Values can be thought of as fingerprints for files. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value – the hash value - is produced that identifies the contents of the file. If the contents are modified in any way, the value of the hash will also change significantly.

b. On April 29, 2017, the UCA was able to directly connect and download approximately 2,711 files from the SUSPECT IP ADDRESS. Between 1:31 p.m. and 5:49 p.m., UCA downloaded files containing images of child pornography and/or child erotica. The SUSPECT IP ADDRESS was the sole candidate for each download, meaning that each file was downloaded directly from the SUSPECT IP ADDRESS.

11. On August 15, 2018, I reviewed the files downloaded by UCA. Based on my training and experience, I believe that the downloaded files contained child pornography and/or erotica. Three of the files are described as follows:

a. **"0yo-g-07-02.jpg"** depicts an image of a hand wrapped around an adult male's penis. The tip of the penis is being held against what appears to be an infant's nude buttocks. There is a creamy substance, which appears to be semen, on the tip of the penis and the infant's buttocks.

b. **"Pthc – Qqaazz1yo – pedo man pudding a chubby baby puss(cute).jpg"** depicts an image of a nude infant female, laying on her back. An adult male is holding his erect penis in his left hand between his second and middle finger. The tip of his penis is placed against the vagina of the infant female. There is a creamy substance, which appears to be semen, on the tip of the penis and on the vagina of the infant female.

Instrumentality Protocol

c. **" - -5yo boy Exelent Cock Sucker.mpg"** depicts a video of a nude prepubescent boy, on his hands and knees on a bed. The prepubescent male then orally copulates an adult male with an erect penis. The video lasts approximately 4-5 seconds.

B. January 22 and February 24, 2018 Download of Suspected Child Pornography from the SUSPECT IP ADDRESS

12. On August 21, 2018, I conducted a query of the SUSPECT IP ADDRESS via a law enforcement databases. Based on this query, I learned that another law enforcement officer acting in an undercover capacity, Undercover Officer B (hereafter, "UCB") conducted an online undercover session with the SUSPECT IP ADDRESS in January 2018. Based on information provided by UCB, I learned the following:

a. On January 22, 2018, UCB saw a BitTorrent user connected to the BitTorrent network using the SUSPECT IP ADDRESS and who had made available for sharing a torrent with the infohash: 04c36c3c08a2fe2be062850ec6dfcbe8460509b5. This torrent referenced 5,616 files, at least one of which was identified as being suspected child pornography.

b. UCB was able to directly connect to and download approximately 270 files from the SUSPECT IP ADDRESS.

c. On January 22, 2018, between 3:38 a.m. and 3:53 a.m., UCB downloaded files containing images of child pornography and/or child erotica. The SUSPECT IP ADDRESS was

Instrumentality Protocol

the sole candidate for each download, meaning that each file was downloaded directly from the SUSPECT IP ADDRESS.

d. I reviewed the files downloaded by UCB. Upon review, I determined that the downloaded files contained child pornography and/or erotica. One of the child pornography files is described as follows:

i. **"1139025982907.JPG"** depicts an image of a nude toddler female, laying on her back. An adult male is holding his erect penis in his left hand between his thumb and first finger. The tip of his penis is placed against the vagina of the female. There is a creamy substance, which appears to be semen, on the tip of the penis and on the vagina of the infant female.

e. On February 24, 2018, UCB saw a BitTorrent user connected to the BitTorrent network using the SUSPECT IP ADDRESS who had made available for sharing a torrent with the infohash: 18cb6437728460bf18a086d2957711372d2. This torrent references 20 files, at least one of which was identified as being a file suspected of being child pornography.

f. On February 24, 2018, UCB was able to directly connect and download approximately 20 files from the SUSPECT IP ADDRESS. Between 7:20 p.m. and 8:16 p.m., on February 24, 2018, UCB downloaded files containing images of child pornography and/or child erotica. The SUSPECT IP ADDRESS was the sole

Instrumentality Protocol

candidate for each download, meaning that each file was downloaded directly from the SUSPECT IP ADDRESS.

g. I reviewed the files downloaded by UCB. Upon review, I determined that the downloaded files contained child pornography and/or erotica. One of the files is described as follows:

i. **"KAIT_5yo girl taking a dick.AVI"** depicts a video of a nude female toddler, approximately 5 years old, laying on her back. An adult male is holding his erect penis in his left hand between his thumb and first finger. The tip of his penis is placed against the vagina of the female. The adult male rubs his penis against the vagina of the female and then penetrates the vagina of the female toddler. The video lasts approximately 1 minute and 26 seconds.

C. Identification of AGUILLON as Subscriber of SUSPECT IP ADDRESS

13. Based on my training and experience, as well as my familiarity with this investigation and conversations with other law enforcement officers, I know the following:

a. According to the American Registry of Internet Numbers ("ARIN"), a database that contains publicly available online records for the time periods of the investigation, specifically on the dates and times UCA and UCB conducted their online sessions, the SUSPECT IP ADDRESS was assigned to AT&T.

Instrumentality Protocol

b. On or about May 15, 2017, in response to administrative subpoenas, AT&T Internet Services Legal Compliance reported that the SUSPECT IP ADDRESS was assigned on April 29, 2017 – the date on which the UCA downloaded the suspected child pornography – to the account of "Jonathan Aguillon" at the SUBJECT PREMISES. The email address associated with the account was theyearofthebore@gmail.com.

c. A check of multiple law enforcement databases and publicly accessible websites indicated that a person by the name of "Jonathan Aguillon," date of birth March 31, 1983 is associated with the SUBJECT PREMISES.

d. On July 14, 2017, TFO Gutierrez conducted surveillance at the SUBJECT PREMISES and saw a black 2010 Chevrolet HHR, California license plate number 6PAT937 ("the Black Chevrolet HHR"), parked in the designated parking area for the SUBJECT PREMISES. Law enforcement subsequently determined that the Black Chevrolet HHR is jointly registered to Mario Ariola Aguillon Jr. and AGUILLON.[2]

[2] I checked law enforcement and public database records and found no indication that Mario Ariola Aguillon Jr. is connected to the SUBJECT PREMISES. Law enforcement searched the California Department of Motor Vehicles and found a recent photograph of Mario Ariola Aguillon Jr. Based on their familiarity with this photograph, at no time while conducting surveillance at the SUBJECT PREMISES did law enforcement see and individual who appeared to be Mario Ariola Aguillon Jr.

e. On or about October 27, 2017, after using a ruse, TFO Gutierrez contacted AGUILLON and AGUILLON told TFO Gutierrez that he resided at the SUBJECT PREMISES.

f. On or about May 3, 2018, TFO Bernell E. Trapp conducted surveillance of the SUBJECT PREMISES and saw the Black Chevrolet HHR parked in the designated parking area for the SUBJECT PREMISES.

g. A check of law enforcement databases show AGUILLON was issued a citation on June 6, 2018, in the above vehicle, and told law enforcement that he resided at the SUBJECT PREMISES.

h. On September 9, 2018, TFO Gutierrez telephoned AGUILLON using AGUILLON's mobile telephone number; which was obtained through a previous conversation TFO Gutierrez had with AGUILLON on October 27, 2017. During the call on September 9, 2018, AGUILLON stated to TFO Gutierrez that he lived at the SUBJECT PREMISES. TFO Gutierrez requested a meeting with AGUILLON, and AGUILLON agreed to the meeting, but no further contact was made on the part of AGUILLON.

i. On September 22, 2018, at approximately 2:50 a.m., TFO Aundria Davis drove by the SUBJECT PREMISES and saw the Black Chevrolet HHR parked in the designated parking area for the SUBJECT PREMISES.

j. On November 29, 2018, law enforcement officers conducted surveillance at the SUBJECT PREMISES and observed AGUILLON departing the SUBJECT PREMISES in the Black Chevrolet HHR.

D. People Who Distribute, Receive, View, and Possess Child Pornography Usually Collect and Store Child Pornography In a Safe Place That They Can Regularly Access

14. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who distribute, receive, view, and possess images of child pornography are often individuals who have a sexual interest in children and in images of children. I believe that AGUILLON has an interest in child pornography and a sexual interest in children. I know from my training and experience that there are certain characteristics common to individuals with these interests:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location, including on personal digital devices maintained on their person. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and/or videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Child pornography received via computer is extremely mobile. Through computer technology, digital files

are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto thumb drives so small that they fit onto a keychain. Just as easily, these files can be copied onto disks, or stored on cellular telephones and other digital devices.

h. Because of the nature of computer data, as described in more detail below, persons who collect and store child pornography likely have that child pornography, or remnants of it, on their digital devices for extended periods of time. For example, even without the user's knowledge, computers can often keep track of websites visited or data that has been downloaded, and store it in temporary "caches" or other files. As a result, even if AGUILLON or another resident of the SUBJECT PREMISES used a digital device or another digital device located elsewhere to access the Internet and child pornography, it is likely that evidence of this access will be found in the SUBJECT PREMISES and/or on AGUILLON's person.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

15. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as

telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, flash or thumb drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information relayed to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult

with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive

could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve

residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently

used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the

absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field,

and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

16. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

17. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation. Based upon my training and experience, I have learned that criminals actively search online for criminal affidavits and search warrants, and disseminate them online to other criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting other potential targets to the existence and nature of the investigation,

thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

VII. CONCLUSION

18. For all the reasons set forth herein, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the violations of the SUBJECT OFFENSES, as described in Attachments B-1 and B-2 will be found in a search of the SUBJECT PREMISES, as described in Attachment A-1, and/or on the person of AGUILLON, as described in Attachment A-2.

JAMES DECELLO
Task Force Officer, Federal Bureau of Investigation

The magistrate judge has viewed the images/videos described in paragraphs 16a & b, above, that the affiant alleges are lascivious and, thereafter, placed them inside a sealed envelope and initialed across the seal. The affiant has taken custody of the envelope and will maintain custody until all appeals have been exhausted.

Subscribed to and sworn before me this _____ of December 2018.

UNITED STATES MAGISTRATE JUDGE